WHAT IS CLAIMED IS:

1. A set of one or more analyzers to govern the analysis of information gathered from nodes or groups of nodes as well as the selective production of issue information, the analyzers comprising:

one or more analyzers which govern the analysis of specific configuration information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is configured properly;

one or more analyzers which govern the analysis of specific information resulting from testing to determine whether the tested software and/or hardware associated with a node and/or a group of nodes is functioning properly;

one or more analyzers which govern the analysis of specific diagnostic and/or log information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is functioning properly; and

these analyzers also govern the determination of whether and, if so, of what specific issue information is to be produced.

2. A set of one or more analyzers in accordance with claim 1, further comprising:

a harness or framework which, when provided with a list of one or more of the analyzers and with a list of one or more nodes or groups of nodes, exercises one or more of the analyzers against specific data associated with each node or group of nodes, captures any issue information produced, and augments such issue information with node identification information to produce an issues database.

3. A set of one or more analyzers in accordance with claim 1 wherein at least some analyzers include a code portion and a descriptor portion, the descriptor portion containing information identifying at least some of the specific node information required for the performance of the analysis defined by the code portion.

4. A set of one or more analyzers in accordance with claim 3 wherein at least some analyzers further include a template portion, the template portion defining the format of at least some specific issue information that may be generated as a result of the performance of the analysis defined by the code portion.

5. A set of one or more analyzers in accordance with claim 1 wherein at least some analyzers include a code portion and a template portion, the template portion defining the format of at least some specific issue information that may be generated as a result of the performance of the analysis defined by the code portion.

6. A set of one or more analyzers in accordance with claim 1 wherein the analyzers which govern the analysis of specific configuration information include:

at least one analyzer that analyzes the primary and secondary boot disks of one or more nodes, insuring that the boot disks are not installed on the same path and that their configurations are logical.

7. A set of one or more analyzers in accordance with claim 1 wherein the analyzers which govern the analysis of specific configuration information include:

at least one analyzer that analyzes the standard and backup kernel files of one or more nodes, insuring that the kernel files are not installed on the same path and that their configurations are logical.

8. A set of one or more analyzers in accordance with claim 1 wherein the analyzers which govern the analysis of specific configuration information include:

at least one analyzer that analyzes the configuration of service guard or equivalent software which software performs functional analyses of at least one mission critical switch guard or equivalent node cluster and which software switches one or more tasks from node to node within such a cluster to keep mission critical tasks running.

9. A set of one or more analyzers in accordance with claim 1 wherein the analyzers which govern the analysis of specific configuration information include:

at least one analyzer that analyzes the configuration of one or more hardware devices associated with a node or group of nodes.

10. A set of one or more analyzers in accordance with claim 1 wherein the analyzers which govern the analysis of specific configuration information include:

at least one analyzer that analyzes the system dump configurations of one or more nodes to see that the nodes are configured correctly to enable the performance of a successful system dump in case of a system crash or other failure.

11. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers which govern the analysis of specific diagnostic and/or log information include:

at least one analyzer that analyzes memory error indication information from one or more nodes to determine if memory error conditions are present and, if so, are serious enough to require attention.

12. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers which govern the analysis of specific diagnostic and/or log information include:

at least one analyzer that analyzes at least some data retrieved from a circular buffer containing diagnostic information and/or error messages.

13. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers which govern the analysis of specific diagnostic and/or log information include:

at least one analyzer that analyzes system logging file entries.

14. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers which govern the analysis of specific diagnostic and/or log information include:

at least one analyzer that analyzes an error log of I/O errors.

15. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers which govern the analysis of specific diagnostic and/or log information include:

at least one analyzer that examines and analyzes information extracted from CPU hardware logs of each processor installed upon a node.

16. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes disk usage data to determine the likelihood of "disk full" conditions occurring soon.

17. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes data indicating whether the service guard related daemons or their equivalents are operating properly to insure the continuance of mission critical tasks.

18. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes the operational status of at least one service guard or equivalent cluster of nodes, signaling an issue if such a cluster is down, or if one or more tasks of such a cluster is not running, or if no alternative node is available to which one or more tasks may be switched.

19. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes the status of one or more file systems.

20. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which data relating to the CPUs to determine if any have been de-configured.

21. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes the status of the CPU fans.

22. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes the status of the CPU power supplies.

23. A set of one or more analyzers in accordance with claim 1 wherein the one or more analyzers that govern the analysis of specific information resulting from testing includes:

at least one analyzer which analyzes the output generated by i/o device scans.

24. A method of analyzing information gathered from nodes or groups of nodes and selectively producing issue information, the method comprising:

analyzing one or more specific sets of configuration information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is configured properly;

analyzing one or more specific sets of information resulting from testing to determine whether the tested software and/or hardware associated with a node and/or a group of nodes is functioning properly;

analyzing one or more sets of specific diagnostic and/or log information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is functioning properly; and

determining whether and, if so, what specific issue information is to be produced as a result of these analyses, and producing that issue information.

25. A method of analyzing in accordance with claim 24, further comprising:

providing a list of one or more analyses and a list of one or more nodes or groups of nodes;

performing one or more of the listed analyses against specific data gathered from each listed node or group of nodes; and

capturing any issue information produced and augmenting such issue information with node identification information to produce an issues database.

26. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of configuration information includes:

analyzing the primary and secondary boot disks of one or more nodes to insure that the boot disks are not installed on the same path and that their configurations are logical.

27. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of configuration information includes:

analyzing the standard and backup kernel files of one or more nodes to insure that the kernel files are not installed on the same path and that their configurations are logical.

28. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of configuration information includes:

analyzing the configuration of service guard or equivalent software which software performs functional analyses of at least one mission critical switch guard or equivalent node cluster and which software switches one or more tasks from node to node within such a cluster to keep mission critical tasks running.

29. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of configuration information additionally comprises:

analyzing the configuration of one or more hardware devices associated with a node or group of nodes.

30. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of configuration information additionally comprises:

analyzing the system dump configurations of one or more nodes to see that the nodes are configured correctly to enable the performance of a successful system dump in case of a system crash or other failure.

31. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more sets of specific diagnostic and/or log information aditionally comprises:

analyzing memory error indication information from one or more nodes to determine if memory error conditions are present and, if so, are serious enough to require attention.

32. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more sets of specific diagnostic and/or log information additionally comprises:

analyzing at least some data retrieved from a circular buffer containing diagnostic information and/or error messages.

33. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more sets of specific diagnostic and/or log information additionally comprises:

analyzing system logging file entries.

34. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more sets of specific diagnostic and/or log information additionally comprises:

analyzing an error log of I/O errors.

35. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more sets of specific diagnostic and/or log information comprises:

analyzing information extracted from CPU hardware logs of each processor installed upon a node.

36. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing disk usage data to determine the likelihood of "disk full" conditions occurring soon.

37. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing data indicating whether the service guard related daemons or their equivalents are operating properly to insure the continuance of mission critical tasks.

38. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing the operational status of at least one service guard or equivalent cluster of nodes, signaling an issue if such a cluster is down, or if one or more tasks of such a cluster is not running, or if no alternative node is available to which one or more tasks may be switched.

39. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing the status of one or more file systems.

40. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing data relating to the CPUs to determine if any have been de-configured.

41. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing the status of the CPU fans.

42. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyze the status of the CPU power supplies.

43. A method of analyzing information in accordance with claim 24 wherein the step of analyzing one or more specific sets of information resulting from testing additionally comprises:

analyzing the output generated by i/o device scans.

44. A set of one or more analyzers to govern the analysis of information gathered from nodes or groups of nodes as well as the selective production of issue information, the analyzers comprising:

one or more configuration information analyzer means for analyzing specific configuration information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is configured properly;

one or more test information analyzer means for analyzing specific information resulting from testing to determine whether the tested software and/or hardware associated with a node and/or a group of nodes is functioning properly;

one or more diagnostic and/or log information analyzer means for analyzing specific diagnostic and/or log information to determine whether the software and/or the hardware associated with a node and/or a group of nodes is functioning properly; and

issue information production means for determining whether and, if so, for determining what specific issue information is to be produced.